Zoom: ¿Cómo utilizar las videollamadas de forma segura?

25/04/2020

Las videollamadas de Zoom eran un servicio conocido por un grupo limitado de usuarios que necesitaban realizar de forma sencilla reuniones virtuales convideo de alta calidad desde su aparición en 2012. Sin embargo, la pandemia de coronavirus covid-19 obligó a muchos gobiernos, organismos, empresas y profesionales independientes, entre muchas otras personas, a utilizar esta plataforma para diversas actividades, desde las clases escolares y universitarias a los talleres de yoga y los encuentros laborales.

Así fue como Zoom pasó de tener 10 millones de usuarios a 200 millones en solo tres meses , y la compañía fue víctima de este éxito repentino, con graves fallas de seguridad y privacidad que promete resolver en 90 días. A pesar de estos incidentes, en el camino, las videollamadas grupales de la compañía liderada por Eric Yuan no se detuvieron y ya cuentan con 300 millones de usuarios.

Denuncias de robos de datos bancarios

Con la popularidad de un servicio online que atrae a millones de usuarios también llegan los delincuentes informáticos, ávidos por obtener información personal para cometer otros robos y delitos, con prácticas como el zoombing (entrar a una conferencia ajena para molestar) . Ya aparecieron casos locales de gente que dice que por estar usando Zoom (y dejarlo activo cuando no está en uso, que es algo no recomendable) alguien tuvo acceso a su cuenta bancaria o de MercadoPago. Aunque no está demostrado que haya una relación directa, Zoom

es una aplicación que en un principio era muy insegura (Google prohibió su uso en la compañía), aunque esta semana publicó una nueva versión que, dice, resuelve todos sus problemas.

Para evitar ser víctimas de estos y otros posibles ataques hay que tomar los recaudos necesarios.

Actualizar, si ya la tiene instalada

La más reciente versión de Zoom (publicada esta semana) usa encriptación de sus datos de extremo a extremo y corrige múltiples vulnerabilidades que permitían a alguien tanto entrar a salas ajenas, como capturar información transmitida en una sesión. Esto, en teoría, ahora queda descartado. Así que actualizar es fundamental para proteger los datos propios y de los demás usuarios.

Fundamental: no repetir contraseña

Este es uno de los consejos más importantes, y se aplica tanto a Zoom como a muchas otras cuentas de servicios online: hay que usar una contraseña única . La reutilización de claves es una peligrosa puerta de entrada para los delincuentes digitales, ya que es muy probable que la combinación reciclada esté expuesta en muchos otros ataques informáticos previos.

A modo de referencia, en 2016 Yahoo confirmó que sufrió un ciberataque masivo que expuso más de 1000 millones de cuentas . Un año más tarde hubo una gigantesca filtración de 560 millones de contraseñas robadas de ataques informáticos que sufrieron empresas como LinkedIn, Dropbox, Lastfm, MySpace y Adobe, entre otras.

Esta es una pequeña muestra que reutilizar la misma contraseña es una pésima idea : los delincuentes digitales tienen todos estos registros de ataques informáticos previos con el objetivo de ingresar con la modalidad de prueba y error en los perfiles de redes sociales, correos electrónicos, cuentas bancarias y en todas las plataformas disponibles de Internet.

El antecedente más fresco ocurrió con la app de videollamadas Houseparty , que recibió quejas de usuarios que habían perdido el acceso a sus cuentas de PayPal, Netflix y Spotify, entre otros servicios. Epic Games, los administradores de la aplicación, negó estar vinculada con el robo de cuentas , aseguró que no sufrió una brecha de seguridad y recomendó que los usuarios no utilicen la misma contraseña para diferentes servicios.

Para estos casos, una buena medida es renovar de forma periódica las contraseñas , al menos los servicios más importantes y valiosos, como los correos electrónicos, las redes sociales y las cuentas bancarias. En muchos casos, esta gestión suele ser engorrosa y puede exceder la capacidad de memorización de combinaciones de las personas, pero para estos casos existen los gestores de contraseñas : basta con recordar solo una clave para administrar de forma regular las combinaciones del resto de las cuentas online. En estos casos solo basta con copiar o pegar desde servicios como 1 Password, LastPassword o con programas de código abierto y uso sin costo comoKeePassX .

Confirmar el lugar de descarga de la app

Este es otro consejo que también se aplica a cualquier otro servicio digital, porque la falsificación de programas y aplicaciones es otra técnica utilizada muy a menudo por los delincuentes informáticos. En estos meses, debido a la popularidad de uso de los software de videollamadas, solo hay que descargar los programas de sitios oficiales .

En el caso de Zoom, el sitio oficial es www.zoom.us para descargar de forma segura el programa oficial para Windows y Mac, mientras que para los dispositivos móviles la aplicación está disponible en las tiendas App Store de Apple y Play Store de Google.

Dados los problemas que tuvo Zoom en el último mes, siempre actualice el programa a la última versión disponible. En el caso de la versión para Windows o Mac, el software realizará una notificación, mientras que en los teléfonos móviles y tabletas se deberá verificar la tienda de aplicaciones.

Conozca las funciones de Zoom para protejer sus reuniones virtuales

Por su facilidad de uso, Zoom se convirtió en una opción muy popular para realizar las videollamadas. Sin embargo, esta virtud se transformó en una vulnerabilidad con personas que vandalizaban las reuniones virtuales. En pos de promover un uso sencillo de la herramienta, sus creadores dejaron muchas configuraciones predeterminadas a la merced de estas visitas indeseadas.

Estos son ajustes específicos de Zoom que están disponibles en la sección de configuraciones y que vale la pena repasar para evitar problemas en las videollamadas grupales. Tómese un tiempo para conocer las funciones de Zoom para evitar la exposición a situaciones no deseadas.

No comparta el enlace de Zoom en las redes sociales: el acceso a una reunión en Zoom se puede realizar desde un link web, una modalidad que facilita mucho el uso de las videollamadas. Sin embargo, hay que evitar exponer este acceso de forma pública para evitar la intrusión de personas no deseadas. Zoom también permitía utilizar un identificador personal de las reuniones para facilitar un encuentro virtual tenía que realizarse de forma periódica. Sin embargo, la mejor opción es que este

código se renueve de forma aleatoria con cada convocatoria.

Reuniones protegidas con una clave: poner una contraseña a la reunión es la mejor forma de asegurar que la videollamada cuente solo con las personas que fueron invitadas. Esta fue una de las opciones que Zoom activó de forma predeterminada. Y, por supuesto, tampoco es una buena idea exponer esta combinación de forma pública, al igual que los links de las reuniones.

Sala de espera: como su nombre lo indica, deja a los participantes de la videollamada en una lista de espera, una función muy buena que permite que el administrador del encuentro aprobar los ingresos a la reunión virtual de forma manual, y verificar quién es la persona que está entrando a la reunión. Este es otro ajuste que Zoom acaba de activar de forma automática al crear una videollamada grupal.

Solapa Seguridad: este acceso directo disponible en la barra de herramientas de Zoom permite bloquear la reunión de forma rápida ante un problema en la videollamada, para que nadie ingrese a la reunión virtual. También se puede habilitar o limitar el uso de compartir pantalla, chatear o renombrar los nombres de usuario para evitar interrupciones no deseadas.